Wireless Network Security

The Enemy is Listening

Written By

David Childers

www.ScenicRadio.Com

Relaxing Entertainment for the World

www.BroadcastingWorld.Com

Global Broadcast Information Portal

Creative Common License

Cover graphic - Antenna And Radio Waves clip art.
www.clker.com/clipart-23862.html

Foreword graphic -Bronze skeleton key clip art.
www.wpclipart.com/tools/locks/keys/bronze_skeleton_key.png

About The Author

David Childers is the Content Manager for the Global Broadcasting portal www.BroadcastingWorld.com. He is very active in the Internet broadcast industry and has written numerous guides and a book about this growing technological field. He is also the webmaster of www.ScenicRadio.com, the global destination for relaxing entertainment.

Mr. Childers' work has been cited in several national and International publications, including these:

Five Essays on Copyright In the Digital Era
Turrer Publishing

Research On High-Profile Digital Video Production
Digital Content Association of Japan

Video Podcasting in Perspective: The History, Technology, Aesthetics and Instructional Uses of a New Medium
Journal of Educational Technology Systems

Video Podcasting: When, Where and How it's Currently used for Instruction
The National Convention of the Association for Educational Communications and Technology

IP Packet Charging Model For Multimedia Services
National University of Rwanda

Preservation of audiovisual mediums: Problems and challenges.
Platform for Archiving and Preservation of Art on Electronic and Digital Media.

P2P Technology Trend and Application to Home Network
Electronics and Telecommunications Research Institute Journal

Peer To Peer Computing - The Evolution of a Disruptive Technology
Idea Group Publishing

Peer-to-Peer Systems and Applications
Lecture Notes In Computer Science
Springer Berlin / Heidelberg

Feedback

Please feel free to contact the author if you have any questions or comments. Your feedback is greatly appreciated.

You can contact the author here: www.KL7AF.com

Foreword

Wireless networking can give you the freedom of movement and the ability to stay connected. It can also be an open door for unscrupulous people to gain access to personal information that may be exchanged over a wireless Internet connection.

It is important that the reader use this information to understand the importance of wireless network security and ensure that the necessary precautions are taken.

I would like to thank Scarlet Coker for providing assistance with the editing of this guide.

It is my sincere hope that the reader finds this information guide beneficial.

David Childers

August 20, 2010

Posveèeno Neži Vidmar.
Sanje so želje srca.

Knowledge Is The Key

When you know that you're capable of dealing with whatever comes, you have the only security the world has to offer.

Harry Browne

Index

The Importance Of Wireless Network Security

Security is the ability to guard against damage, threats, and criminal action. It is important to actively pursue a plan that creates and / or enhances security.

Protecting yourself against vulnerabilities is never a one-step procedure, it must be a continuing process for both the wireless network administrator and wireless access network user. Both must incorporate thorough security practices and stay informed of current security issues / vulnerabilities. Both physical security and encryption security are important to the wireless network administrator and to the end user.

A wireless network manager for a business or organization needs to educate and train all users. They should be made aware of security measures that have been put into place and why they were implemented. It is also important to routinely check with the Human Relations and Department Head personnel to validate network access for employees and access levels for network / computer systems.

Wireless networking is ideal for allowing people to remotely connect to the Internet without being “tied down” by the need for physically connecting to a network. In todays fast paced world, having convenient access to business or personal data is important, however, it is important to understand the risks involved in managing and use of wireless networks. It is essential to implement and use security measures to prevent unauthorized access to the wireless network. Information or resources can be compromised when using wireless network connections without implementing and using security procedures .

Hackers and data thieves do not require much information for ill gain. They can gather information over time; and as information is gathered, it can be collated and analyzed for use against a selected target.

It is important to document the wireless network security plan that is being used. This will allow the wireless network administrator and management to have the ability to routinely review the procedures. This documentation must also be readily available to authorized individuals should there be unforeseen events that require access to that information. Wireless network documentation, technical information, password and hardware access must be secured and properly stored to prevent unauthorized persons from accessing that information.

An alternate individual should be designated as a wireless network manager in the event that the primary person responsible for the wireless network is not readily accessible. They must also have the ability to gain immediate access to any documentation, plans or information related to the wireless network. This will allow designated personnel the ability to immediately respond to any unforeseen events that may occur.

What Is Wireless Networking

Wireless networking is the use of radio frequency technology to connect computers with other remote computers or networks. It requires the use of both receiver and transmitter equipment to establish a full duplex communications link. Wireless networking can provide short, medium, or long range data exchange, depending on the hardware used.

Wireless networking employs several methods for data communications that can be utilized by different hardware platforms. These specialized processes provide unique data formats, authentication processes, error detection and correction capabilities to guarantee communications.

802.11

This protocol is an Institute of Electrical and Electronics Engineers (IEEE) International standard used for Local Area Network (LAN) computer communications.

This group of protocols use a form of Adaptive Coding and Modulation (ACM) to optimize data exchange over a wireless network connection. These protocols also include the ability to adjust the communication characteristics to match the communication conditions encountered. Such conditions include: signal interference, amount of data loss, receiver sensitivity or transmitter power.

Different countries or geographic organizations maintain unique channel assignments for their individual 802.11 wireless network communication services. All countries however, have adopted IEEE recommendations for establishing a uniform center frequency and signal attenuation levels outside of each data channel.

Protocol	Frequency	Bandwidth
802.11 [1] [2]	2.4 GHz - ITU Band 9	20 MHz
802.11 a [3]	3.7 GHz - ITU Band 9 / 5 GHz - ITU Band 10	20 MHz
802.11 b [1]	2.4 GHz - ITU Band 9	20 MHz
802.11 g [1] [3]	2.4 GHz - ITU Band 9	20 MHz
802.11 n [3]	2.4 GHz - ITU Band 9 / 5 GHz - ITU Band 10	20 MHz / 40 MHz

ITU - International Telecommunications Union

Modulation Methods

[1] - Direct Sequence Spread Spectrum
The transmitted data is spread over the entire frequency, regardless of the amount of data being sent.

[2] - Frequency Hopping Spread Spectrum
The transmitted data modulation carrier is rapidly switched among many frequencies / channels.

[3] - Orthogonal Frequency-Division Multiplexing
The transmitted data signals are assigned non-overlapping individual carrier frequency ranges.

Data Transfer Rate

Protocol	Maximum Theoretical Data Transfer Value
802.11	2 Megabits Per Second
802.11 a	54 Megabits Per Second
802.11 b	11 Megabits Per Second
802.11 g	54 Megabits Per Second
802.11 n	72.2 / 150 Megabits Per Second

3G

This is the Third generation standard for mobile digital devices. This standard provides the following mobile wireless services: telephone, Internet connectivity, video calls, and television. It also provides simultaneous voice and data access with a maximum data rate transfer of 200 Kbits. The KASUMI block cipher is used for network authentication.

4G

This is the Fourth generation standard for mobile digital devices and provides a secure method of data communications using IP networking. This standard provides the following mobile wireless services: telephone, Internet connectivity, gaming and streaming multimedia. The planned data transfer rate will be approximately 100 Mbit/s for mobile access and approximately 1 Gbit/s for low mobility local wireless network access. 4G uses Extensible Authentication Protocol (EAP) for data authentication, which employs special data that is exchanged between the client and the authentication server.

Securing Wireless Networks

Methods For Encrypting Wireless Networks

No Encryption
This is obviously not a preferred option if you wish to maintain security within your wireless network.

Wired Equivalent Privacy (WEP)
This protocol has been identified as being weak by cryptographic experts, due to several major security holes that were discovered. These problems include encryption key size, the possibility of Initialization Vector collisions and altered packets. An encrypted WEP network connection can be easily cracked and decoded with readily available software within a matter of minutes. **IT IS HIGHLY ADVISABLE THAT WEP ENCRYPTION IS NOT USED.**

Wi-Fi Protected Access (WPA)
This protocol was created to update WEP security for devices without the need for replacing legacy hardware. WPA incorporated three important features to resolve the security issues discovered in WEP.

Wi-Fi Protected Access (WPA2)
WPA2 was designed to replace WPA and utilizes an Advanced Encryption Standard (AES) in which both keys and blocks use 128 bits for data encryption. WPA2 also required the design of new hardware to utilize these enhancements.

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)
This protocol was designed for home and small networks that do not require elaborate authentication architecture. Each device connected to the wireless network encrypts the exchanged data using a 256 bit cryptographic key.

Wireless Encryption Key Password Recommendation

- Change the default password setting for the encryption key used by the wireless network router.
- This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.
- Establish a routine for changing the encryption key password for the wireless network router.
- It is vital that any password information is documented and stored in a secure method.
- DO NOT USE ANY DEFAULT PASSWORD SETTING.

Wireless Router Administration Password Recommendation

- Change the default password setting for the administrator access to the wireless network router.
- This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.
- Establish a routine for changing the administrative password for the wireless network router.
- It is vital that any password information is documented and stored in a secure method.
- DO NOT USE ANY DEFAULT PASSWORD SETTING.

Safeguard Wireless Network Password Information

It is important to educate and Inform all persons that access a business or organizational wireless network that they must safeguard the network access password information. It is imperative they understand the wireless network can be compromised and valuable data can be lost if they misuse this information.

SSID (Service Set Identifier)

The SSID is an identification marker added to all packets broadcast within a wireless network. The purpose of the identification marker is to identify each packet as belonging to a specific wireless network.

DO NOT USE ANY DEFAULT SSID IDENTIFICATION SETTINGS. The SSID identification should contain both numbers and letters, in addition to using a minimum of 10 letters for the identification. It is highly recommended that ordinary phrases or names are not used for the SSID.

The SSID broadcast announces the presence of a wireless network router. Turning off the SSID feature will disable the ability of people to casually detect the presence of the wireless network router.

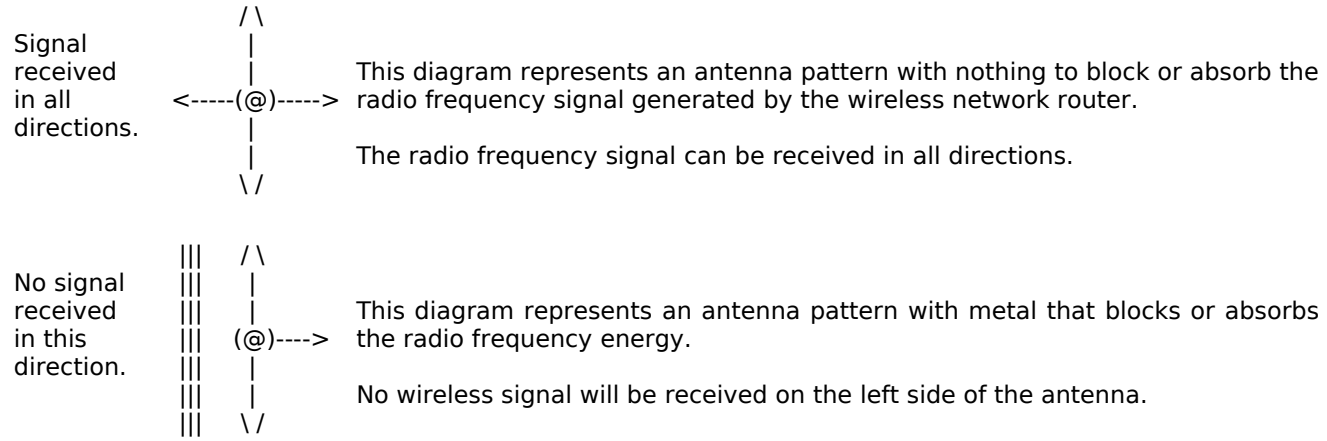
Disable Dynamic Host Configuration Protocol (DHCP) And Use Static IP Addresses

Selecting the Static IP addressing option will require any computer attempting to connect with the wireless network access point to manually configure the network settings. This will help prevent unauthorized use of the wireless network access point. The assigned static IP addresses should be selected from the standard private IP address ranges.

The DHCP configuration automatically assigns an IP address to a computer when it joins a wireless network. There is no manual administration needed, which allows any computer accessing the network to automatically be configured.

Limit Radiation Pattern Of Antenna

Radio waves generated between 2.5 - 5 GHz are very directional. Large pieces of aluminum or sheet metal can be placed around the transmitting antenna to prevent signals from propagating to areas that will not be used by any participants in the wireless network.



Antenna Recommendations

- Low gain transmission antennas can be used to decrease the radio frequency power and decrease the overall effective operating area of the wireless network.

- High gain transmission antennas can be used with the wireless network to increase the radio frequency power and improve the overall effective operating area of the wireless network.

- Special antennas can be used to control the antenna pattern, which directly affects which directions the wireless network data is sent.

- The wireless network router antenna should be located in a centralized area to maximize the access coverage area. It is also important to ensure there are no surrounding obstructions, such as other equipment, to block the signal for the wireless network users.

Decoy Access Points

These are also known as honeypots, which can be deployed as surveillance and early warning tools. The access logs can be reviewed to check for unauthorized access attempts. Decoy access points should not be connected with any production network or computer system. These decoy access points could be used by an attacker to break into the network and connected computers without proper precautions.

Additional Security Recommendations Include:

- Keep firmware up to date on all wireless network equipment.
- Turn off the wireless network equipment after business hours.
- Restrict access to the wireless network by computer MAC address.
  * A Media Access Control address (MAC address) is a unique alpha-numeric identification that are assigned to network adapters or network interface cards. These are usually designated by the hardware manufacturer for individual computer system identification.

- Incorporate or activate firewall protection within the wireless router.
- Use a data filter to block out designated content by protocol, type, or web address / IP addresses.
- Limit and secure physical access to the wireless router.
- Limit and secure administrative access to the wireless router.

Recommendations For Personal Wireless Network Use

You should follow these security recommendations when connecting to the Internet through a wireless network access point:

- Keep your computer system and installed software up to date.
- Install and properly configure a firewall on your computer.
- Install and properly configure virus and malware detection / removal software on your computer.
- Use a SAFE WEB BROWSER.
- Use EXTREME CAUTION when using open or public wireless access points.
  (NEVER ASSUME an open or public wireless access point is using data encryption.)
- Use ADDITIONAL NETWORK DATA ENCRYPTION.

Using additional data network encryption provides a second layer of security in addition to the encryption processes used by the wireless network.

Virtual Private Networks (VPN) encrypt and encapsulate data that is exchanged between devices located at remote locations or on separate networks. This encryption is achieved through the use of advanced cryptographic methods, which prevents the data from being analyzed while it is being exchanged.

VPN Tools:

Tor

This software anonymizes the origin of Internet traffic, and encrypts the data traveling between the computer it is installed on and the Tor network. This software DOES NOT encrypt traffic between the Tor network and the final destination.

(Available as a FREE Firefox plugin.)
www.torproject.org/download.html

Additional FREE VPN software

www.techpp.com/2009/07/09/top-5-free-vpn-clients/
www.avinashtech.com/internet/15-best-free-vpn-for-secure-anonymous-surfing/

Secure Socket Layer Connections

Use SSL for website interaction when possible. This is a cryptographic protocol that provides additional security for communications over the Internet. This type of Internet communication is characterized by the inclusion of a **S** following the **HTTP** URL designator.

Example: **HTTPS**://www.google.com

SSL Tools:

HTTPS Everywhere

This is a FREE Firefox extension that encrypts computer network communications with a number of major websites.
www.eff.org/https-everywhere

Equipment Safety

Antenna Ground

It is important to properly ground any outdoor antennas that are used with wireless access network devices. This will provide protection against damage due to lightening or electrostatic build up.

Uninterruptible Power Supply

The wireless network equipment should be connected to a back up power source, such as an uninterrupted power supply. This will maintain network function and performance if the primary power supply is interrupted. Frequent or rapid power drops can also damage electronic equipment.

Adequate Equipment Ventilation

Any electronic equipment that is secured in protected enclosures must have adequate ventilation. Large amounts of electronic equipment can generate very high temperatures that can degrade equipment performance or cause system failure.

Breaking Wireless Networks

This basic information is presented to show the ease of selecting and acquiring wireless network access points for future analytical evaluation.

Electronic Order Of Battle

This is a system that is used by military Signal Intelligence personnel to gather and process information on selected targets of interest. These same attributes are used by individuals seeking to gain unauthorized access to wireless networks. This collection of information can be cataloged and used at a later time.

This information includes:

- Site designation: SSID.
- Nomenclature: Equipment type.
- Location: Physical location of access point.
- Site function: Does access point require authentication?
- Other pertinent information obtained that has significance when related to the access point:
  * Hours of availability.
  * Encryption method used.
  * Antenna RF pattern plot.
  * Full, limited Internet access, or Internal network access.
  * Relative bandwidth available.
  * Is this a primary signal source or a secondary signal source?

Software has been developed that can be used to locate and monitor wireless access points, in addition to cracking / breaking encryption methods used to secure wireless access points.

Additional tools can also be used to simply locate wireless network access points. Once these access points are located and identified, they can be electronically reconnoitered at a later time to gain additional information.

Disruption Or Jamming Of Wireless Networks

Degrading a wireless network signal can be initiated to force the network manager of a wireless network access point to re-configure their equipment or change settings to overcome the attack.